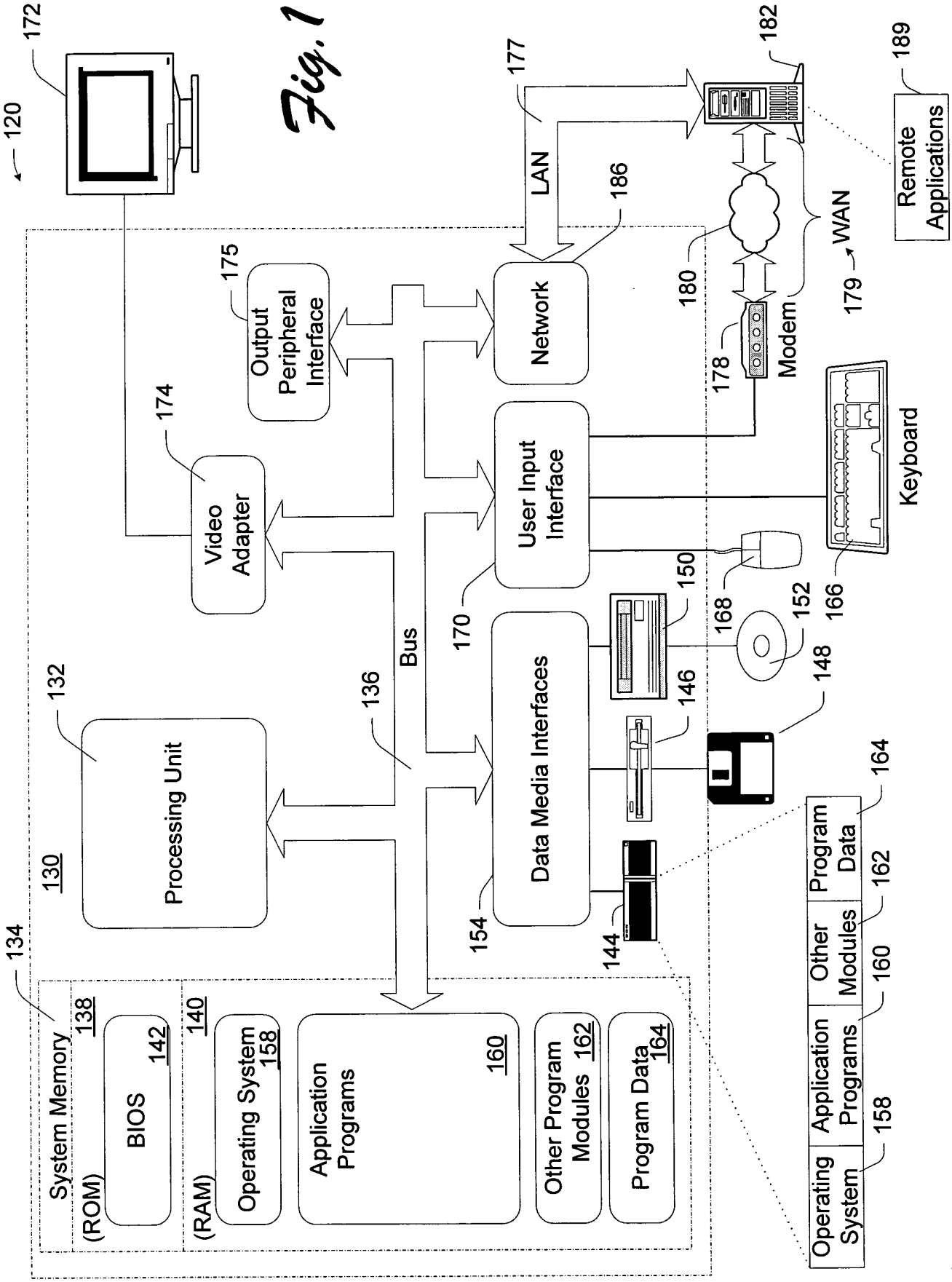
120
172
Fig. 1
177
182
189
LAN
WAN
Remote Applications
186
180
179
175
Output Peripheral Interface
Network
Modem
178
174
Video Adapter
User Input Interface
Keyboard
Bus
170
168
166
150
152
132
136
Processing Unit
Data Media Interfaces
146
148
130
154
144
134
System Memory
138
(ROM)
BIOS
142
140
(RAM)
Operating System
158
Application Programs
160
Other Program Modules
162
Program Data
164
Operating System
158
Application Programs
160
Other Modules
162
Program Data
164

200

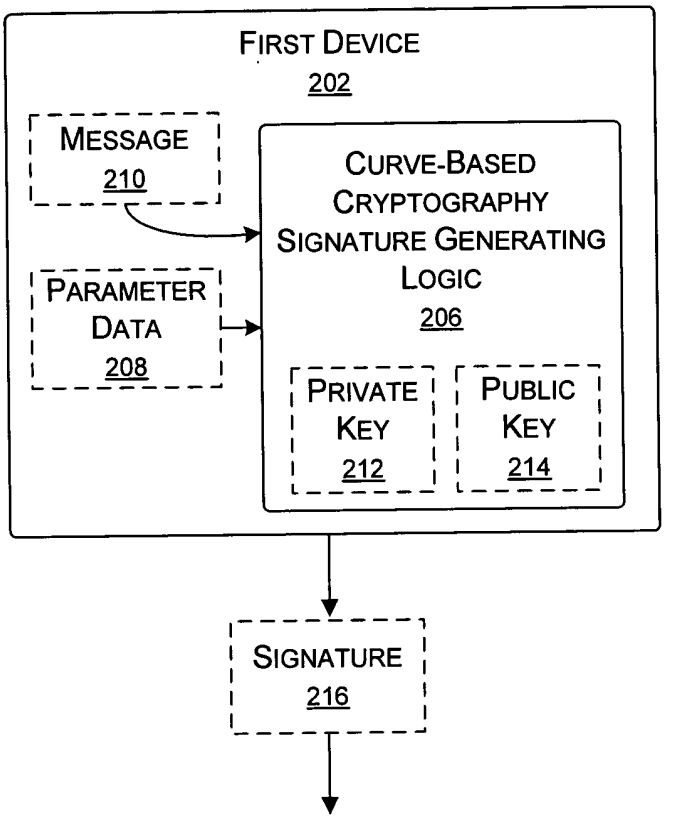
FIRST DEVICE
202
MESSAGE
210
PARAMETER DATA
208
CURVE-BASED CRYPTOGRAPHY SIGNATURE GENERATING LOGIC
206
PRIVATE KEY
212
PUBLIC KEY
214
SIGNATURE
216
SECOND DEVICE
204
MESSAGE
210
PARAMETER DATA
208
PUBLIC KEY
214
CURVE-BASED CRYPTOGRAPHY SIGNATURE VERIFYING LOGIC
218

Fig. 2

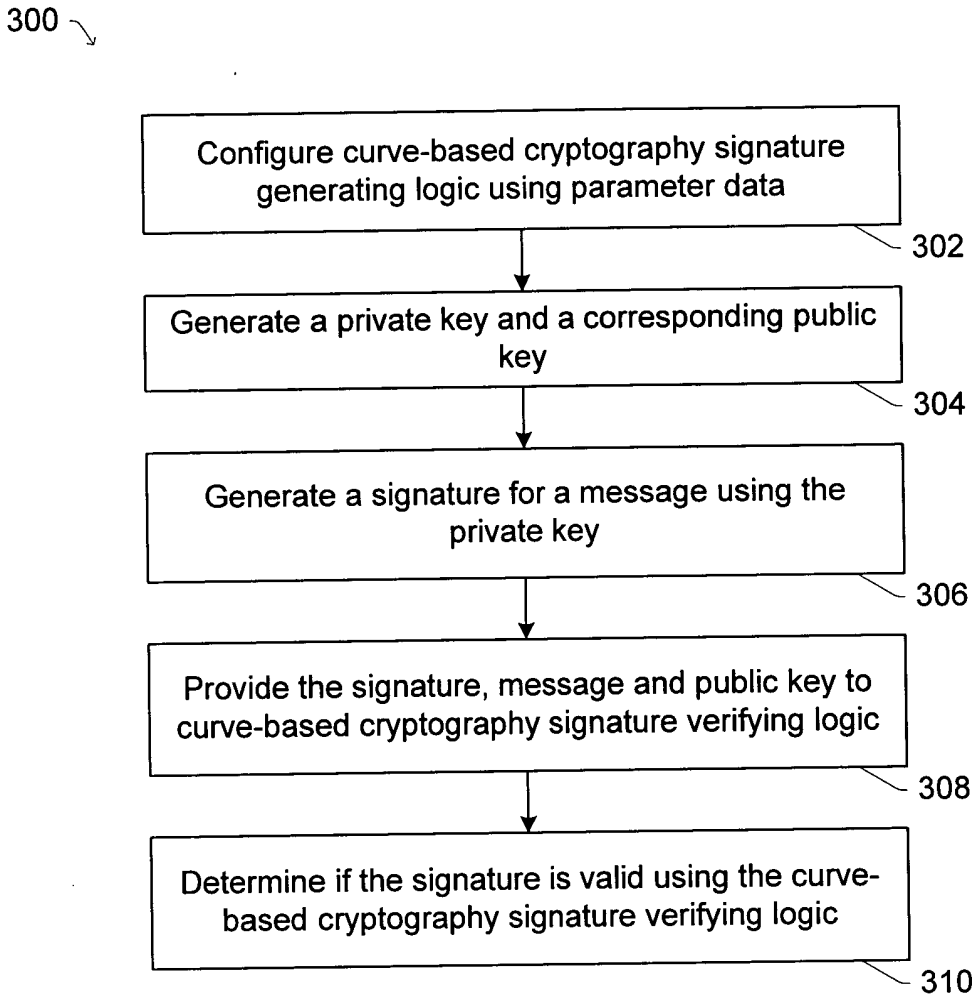
300
Configure curve-based cryptography signature generating logic using parameter data
302
Generate a private key and a corresponding public key
304
Generate a signature for a message using the private key
306
Provide the signature, message and public key to curve-based cryptography signature verifying logic
308
Determine if the signature is valid using the curve-based cryptography signature verifying logic
310

Fig. 3